(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 June 2001 (07.06.2001)

PCT

(10) International Publication Number
WO 01/41353 A3

(51) International Patent Classification[7]: H04L 9/08, 29/06

(21) International Application Number: PCT/US00/41995

(22) International Filing Date:
7 November 2000 (07.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/451,504 30 November 1999 (30.11.1999) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, Palo Alto, CA 94303 (US).

(72) Inventors: PERLMAN, Radia; 10 Huckleberry Lane, Acton, MA 01720-3731 (US). HANNA, Stephen; 3 Beverly Road, Bedford, MA 01730 (US).

(74) Agent: PARK, Richard; Suite 201, 508 2nd Street, Davis, CA 95616 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

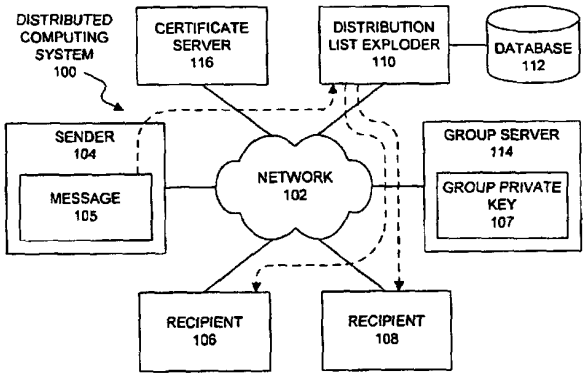
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

(88) Date of publication of the international search report:
21 February 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR SENDING ENCRYPTED ELECTRONIC MAIL THROUGH A DISTRIBUTION LIST EXPLODER



(57) Abstract: One embodiment of the present invention provides a system for sending an encrypted message through a distribution list exploder in order to forward the encrypted message to recipients on a distribution list. The system operates by encrypting the message at a sender using a message key to form an encrypted message. The system also encrypts the message key with a group public key to form an encrypted message key. The group public key is associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message. Next, the system sends the encrypted message and the encrypted message key to the distribution list exploder, and the distribution list exploder forwards the encrypted message to a plurality of recipients specified in the distribution list. After receiving the encrypted message and the encrypted message key, the recipient decrypts the encrypted message key to restore the message key. Next, the recipient decrypts the encrypted message using the message key to restore the message. In a variation on the above embodiment, the recipient decrypts the encrypted message key by sending the encrypted message key from the recipient to a group server, which holds the group private key. The group server decrypts the encrypted message key using the group private key to restore the message key, and returns the message key to the recipient in a secure manner.

WO 01/41353 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/41995

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HERFERT M: "SECURITY-ENHANCED MAILING LISTS" IEEE NETWORK,IEEE INC. NEW YORK,US, vol. 11, no. 3, 1 May 1997 (1997-05-01), pages 30-33, XP000689787 ISSN: 0890-8044	1-6, 10-19, 23-26, 30,31
Y	abstract page 30, right-hand column, line 8 - line 10 page 31, left-hand column, line 13 -right-hand column, line 20 --- -/--	7-9, 20-22, 27-29

[X] Further documents are listed in the continuation of box C. [ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 June 2001	29/06/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Masche, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/41995

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	SERENELLI B ET AL: "SECURING ELECTRONIC MAIL SYSTEMS" SAN DIEGO, OCT. 11 - 14, 1992,NEW YORK, IEEE,US, vol. CONF. 11, 11 October 1992 (1992-10-11), pages 677-680, XP000346673 ISBN: 0-7803-0586-8	7-9, 20-22, 27-29
A	table I page 29.1.1, right-hand column, line 12 -page 29.1.2, right-hand column, line 9 page 29.1.4, left-hand column, line 11 -right-hand column, line 4	1-3,12, 14-16, 25,31
A	TSUTOMU MATSUMOTO ET AL: "ON THE KEY PREDISTRIBUTION SYSTEM: A PRACTICAL SOLUTION TO THE KEY DISTRIBUTION PROBLEM" PROCEEDINGS OF THE CONFERENCE ON THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 7, 1987, pages 185-193, XP000130202 abstract page 186, line 8 - line 40 page 189, line 1 - line 10	1,2,14, 15,25,31